L Number	Hits	Search Text	DB	Time stamp
-	40	chiffrement algorithme	USPAT;	2004/04/27
			US-PGPUB; EPO; JPO;	14:46
-	19565	(encrypt\$4 algorithm\$2) with circuit	DERWENT; IBM_TDB USPAT; US-PGPUB; EPO; JPO;	2004/04/27
_	454	(encrypt\$4 algorithm\$2) with circuit with parallel	DERWENT; IBM_TDB USPAT; US-PGPUB; EPO; JPO;	2004/04/27
_	513	<pre>(encrypt\$4 algorithm\$2) with circuit with (parallel ("same time"))</pre>	DERWENT; IBM_TDB USPAT; US-PGPUB; EPO; JPO;	2004/04/27 14:50
_	615	<pre>(encrypt\$4 algorithm\$2) with circuit with (parallel simultaneous\$3 ("same time"))</pre>	DERWENT; IBM_TDB USPAT; US-PGPUB; EPO; JPO;	2004/04/27
-	304	((encrypt\$4 algorithm\$2) with circuit with (parallel simultaneous\$3 ("same time"))) same (throughput perform\$4 output product\$4 efficien\$4)	DERWENT; IBM_TDB USPAT; US-PGPUB; EPO; JPO; DERWENT;	2004/04/27 14:52
_	8	((encrypt\$4 algorithm\$2) with circuit with (parallel simultaneous\$3 ("same time"))) same (throughput perform\$4 output product\$4 efficien\$4) and	IBM_TDB USPAT; US-PGPUB; EPO; JPO; DERWENT;	2004/04/27
_	23	<pre>(symmetry asymmetry) ((encrypt\$4 algorithm\$2) with circuit with (parallel simultaneous\$3 ("same time"))) same (throughput perform\$4 output product\$4 efficien\$4) and</pre>	IBM_TDB USPAT; US-PGPUB; EPO; JPO; DERWENT;	2004/04/27
	51	<pre>(symmetr\$2 asymmetr\$2) ((encrypt\$4 algorithm\$2) with (circuit appaatus device) with (parallel simultaneous\$3 ("same time"))) same (throughput perform\$4 output product\$4</pre>	IBM_TDB USPAT; US-PGPUB; EPO; JPO; DERWENT;	2004/04/27
-	54	efficien\$4) and (symmetr\$2 asymmetr\$2) ((encrypt\$4 algorithm\$2) with (circuit apparatus device) with (parallel simultaneous\$3 ("same time"))) same (throughput perform\$4 output product\$4	IBM_TDB USPAT; US-PGPUB; EPO; JPO; DERWENT;	2004/04/27
-	29	efficien\$4) and (symmetr\$2 asymmetr\$2)	IBM_TDB USPAT; US-PGPUB; EPO; JPO; DERWENT;	2004/04/27
-	25	efficien\$4) and (symmetr\$2 asymmetr\$2) (((encrypt\$4 algorithm\$2) with (circuit apparatus device) with (parallel simultaneous\$3 ("same time"))) same (throughput perform\$4 output product\$4	IBM_TDB USPAT; US-PGPUB; EPO; JPO; DERWENT;	2004/04/27 15:23
_	67	efficien\$4) and (symmetr\$2 asymmetr\$2)) not (((encrypt\$4 algorithm\$2) with (circuit apparatus device) with (parallel simultaneous\$3 ("same time"))) with (throughput perform\$4 output product\$4 efficien\$4) and (symmetr\$2 asymmetr\$2))	USPAT; US-PGPUB; EPO; JPO;	2004/04/27 15:33

Search History 4/29/04 7:00:43 PM

	10685	((encrypt\$4 algorithm\$2) with circuit with (parallel simultaneous\$3 ("same	USPAT; US-PGPUB;	2004/04/27 15:34
-	6	time"))) and ((data information) with (inaccessible separate isolat\$4 access\$3) with (system)) ((double dual) adj port) ((encrypt\$4 algorithm\$2) with circuit	EPO; JPO; DERWENT; IBM_TDB USPAT;	2004/04/27
		with (parallel simultaneous\$3 ("same time"))) and ((data information) with (inaccessible separate isolat\$4 access\$3) with (system)) and ((double dual) adj port)	US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	15:41
_	12	((encrypt\$4 algorithm\$2) with circuit with (parallel simultaneous\$3 ("same time"))) and (isolat\$4 or separat\$4) and ((double dual) adj (bus memory port))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2004/04/27 15:54
-	111	<pre>((encrypt\$4 algorithm\$2) with (hardware apparatus design system circuit) with (parallel simultaneous\$3 ("same time"))) and (isolat\$4 or separat\$4) and ((double</pre>	USPĀT; US-PGPUB; EPO; JPO; DERWENT;	2004/04/27 16:00
-	67	<pre>dual) adj (bus memory port)) ((encrypt\$4 algorithm\$2) with (hardware apparatus design system circuit) with (parallel simultaneous\$3 ("same time"))) and ((isolat\$4 or separat\$4) with (process\$4 system)) and ((double dual)</pre>	IBM_TDB USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/27 16:01
-	68	adj (bus memory port)) ((encrypt\$4 algorithm\$2) with (hardware apparatus design system circuit) with (parallel simultaneous\$3 ("same time"))) and ((isolat\$4 or separat\$4) with (process\$4 system host computer)) and	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/27 16:28
_	41	<pre>((double dual) adj (bus memory port)) ((encrypt\$4 algorithm\$2) with (hardware apparatus design system circuit) with (parallel simultaneous\$3 ("same time"))) and ((isolat\$4 or separat\$4) with (process\$4 system host computer)) and ((double dual) adj (bus memory port)) and (symmetr\$2 asymmetr\$2 key secret)</pre>	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/27 16:29
-	66		USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/27 16:30
-	63	· · · · · · · · · · · · · · · · · · ·	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/27 16:33
-	56	<pre>((encrypt\$4 algorithm\$2 key cipher) same (hardware apparatus design system circuit) same (parallel simultaneous\$3 ("same time"))) and ((isolat\$4 or separat\$4) with (process\$4 system host computer)) and ((double dual) adj (bus memory port)) and (symmetr\$2 asymmetr\$2 key secret cipher) and ((secur\$3 protect\$3) with (stor\$3 memory)) and (programmable</pre>	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/27 16:35
	<u> </u>	fpga gate logic)		

-	55	((encrypt\$4 algorithm\$2 key cipher) same	USPAT;	2004/04/27
l		(hardware apparatus design system circuit	US-PGPUB;	16:46
i) same (parallel simultaneous\$3 ("same	EPO; JPO;	
		time"))) and ((isolat\$4 or separat\$4)	DERWENT;	
		with (process\$4 system host computer))	IBM TDB	,
		and ((double dual) adj (bus memory		
		port)) and (symmetr\$2 asymmetr\$2 key		1
		secret cipher) and ((secur\$3 protect\$3)		
i		with (stor\$3 memory)) and (programmable		
		fpga gate logic) and ((exchang\$4		
	٠.,	transfer\$4) with (host computer system))		
-	14		USPAT;	2004/04/27
		(hardware apparatus design system circuit	US-PGPUB;	16:37
) same (parallel simultaneous\$3 ("same	EPO; JPO;	
		time"))) and ((isolat\$4 or separat\$4)	DERWENT;	
		with (process\$4 system host computer))	IBM TDB	
		and ((double dual) adj (bus memory		
		port)) and (symmetr\$2 asymmetr\$2 key		
	,	secret cipher) and ((secur\$3 protect\$3)		1
		with (stor\$3 memory)) and (programmable		
		fpga gate logic) and ((exchang\$4		
		transfer\$4) with (host computer system)		
		with pci)		į.
-	23	((encrypt\$4 algorithm\$2 key cipher) same	USPAT;	2004/04/27
		(hardware apparatus design system circuit	US-PGPUB;	16:43
) same (parallel simultaneous\$3 ("same	EPO; JPO;	
		time"))) and ((isolat\$4 or separat\$4)	DERWENT;	
		with (process\$4 system host computer))	IBM TDB	
,		and ((double dual) adj (bus memory	1011_100	
		port)) and (symmetr\$2 asymmetr\$2 key		
		secret cipher) and ((secur\$3 protect\$3)		
		with (stor\$3 memory)) and (programmable		
		fpga gate logic) and ((exchang\$4		İ
		transfer\$4) with (host computer system)		-
		with (interface pci))		
_	0		USPAT;	2004/04/27
		(hardware apparatus design system circuit	US-PGPUB;	16:43
) same (parallel simultaneous\$3 ("same	EPO; JPO;	
		time"))) and ((isolat\$4 or separat\$4)	DERWENT;	
		with (process\$4 system host computer))		
			IBM_TDB	
	ĺ	and ((double dual) adj (bus memory		
		port)) and (symmetr\$2 asymmetr\$2 key		
		secret cipher) and ((secur\$3 protect\$3)		
		with (stor\$3 memory)) and (programmable		
		fpga gate logic) and ((exchang\$4		
		transfer\$4) with (host computer system)		
		with (interface pci))) not (((encrypt\$4		
		algorithm\$2 key cipher) same (hardware		
		apparatus design system circuit) same		
		(parallel simultaneous\$3 ("same time")))		
		and ((isolat\$4 or separat\$4) with		
		(process\$4 system host computer)) and		
		((double dual) adj (bus memory port))		
		and (symmetr\$2 asymmetr\$2 key secret		
		cipher) and ((secur\$3 protect\$3) with		
		(stor\$3 memory)) and (programmable fpga		
		gate logic) and ((exchang\$4 transfer\$4)		
		with (host computer system)))		
		<u> </u>	t	1

_	32	(((encrypt\$4 algorithm\$2 key cipher) same	USPAT;	2004/04/27
		(hardware apparatus design system circuit	US-PGPUB;	16:43
) same (parallel simultaneous\$3 ("same	EPO; JPO;	
		time"))) and ((isolat\$4 or separat\$4)	DERWENT;	
		with (process\$4 system host computer))	IBM TDB	
		and ((double dual) adj (bus memory		
		port)) and (symmetr\$2 asymmetr\$2 key		
		secret cipher) and ((secur\$3 protect\$3)		
		with (stor\$3 memory)) and (programmable		
		fpga gate logic) and ((exchang\$4		
		transfer\$4) with (host computer system)))		
		not (((encrypt\$4 algorithm\$2 key cipher)		
		same (hardware apparatus design system		
		circuit) same (parallel simultaneous\$3		
		("same time"))) and ((isolat\$4 or		
		separat\$4) with (process\$4 system host		
		computer)) and ((double dual) adj (bus		
		memory port)) and (symmetr\$2 asymmetr\$2		
		key secret cipher) and ((secur\$3		
		protect\$3) with (stor\$3 memory)) and		
		(programmable fpga gate logic) and		
		((exchang\$4 transfer\$4) with (host	·	
	ļ	computer system) with (interface pci)))		
_	73	((encrypt\$4 algorithm\$2 key cipher) same	USPAT;	2004/04/27
		(hardware apparatus design system circuit	US-PGPUB;	16:48
) same (parallel simultaneous\$3 ("same	EPO; JPO;	
		time"))) and ((double dual) adj (bus	DERWENT;	
		memory port)) and (symmetr\$2 asymmetr\$2	IBM TDB	
		key secret cipher) and ((secur\$3	_	
		protect\$3) with (stor\$3 memory)) and		
		(programmable fpga gate logic) and		
		((exchang\$4 transfer\$4) with (host		
		computer system))	· .	
-	75	"5682027" "5805712"	USPAT;	2004/04/27
			US-PGPUB;	17:49
			EPO; JPO;	
		•	DERWENT;	
			IBM_TDB	
_	36	5805712.URPN.	USPAT	2004/04/27
				17:45

-	75	(US-6427911-\$ or US-6431443-\$ or	USPAT;	2004/04/27
		US-6453397-\$ or US-6484946-\$ or	DERWENT	17:49
1		US-6488211-\$ or US-6505193-\$ or		
1		US-6507904-\$ or US-6510983-\$ or		
		US-6542610-\$ or US-6633981-\$ or		
1		US-6643374-\$ or US-6647494-\$ or		
		US-6659354-\$ or US-6678825-\$ or		
		US-6687721-\$ or US-6697489-\$ or		
!		US-6700902-\$ or US-6641045-\$ or		
1		US-6629244-\$ or US-6633963-\$ or		
1		US-6401208-\$ or US-6389537-\$ or		
		US-6425522-\$ or US-6427909-\$ or		
!		US-6427910-\$ or US-6571335-\$).did. or		
		(US-6575372-\$ or US-6603857-\$ or		
1		US-6389533-\$ or US-6357665-\$ or		.
1		US-6385723-\$ or US-6357004-\$ or		
		US-6202150-\$ or US-6209098-\$ or		1
		US-6219423-\$ or US-6220510-\$ or		
1		US-6230267-\$ or US-6233685-\$ or		
		US-6260172-\$ or US-6293470-\$ or		
		US-6297789-\$ or US-6317832-\$ or		
		US-6320964-\$ or US-6328217-\$ or		
		US-6354489-\$ or US-6125452-\$ or		.]
		US-6145739-\$ or US-6151677-\$ or		
		US-6151678-\$ or US-6164549-\$ or		
		US-6167551-\$ or US-6181803-\$ or		
		US-6189787-\$).did. or (US-6014442-\$ or		
		US-6021201-\$ or US-6052784-\$ or		
		US-6058478-\$ or US-6070148-\$ or		
		US-6076162-\$ or US-6088450-\$ or		
		US-6091817-\$ or US-6095412-\$ or	1	
		US-6115816-\$ or US-6122625-\$ or		
		US-5905245-\$ or US-5912453-\$ or		ł.
		US-5923018-\$ or US-5949881-\$ or		. [
		US-5974143-\$ or US-6000608-\$ or		
		US-5682027-\$ or US-5805712-\$).did. or		
		(US-6145739-\$ or US-5682027-\$ or		1
1		US-5805712-\$).did.		

- 9628	, , , , , , , , , , , , , , , , , , , ,	USPAT;	2004/04/27
	US-6453397-\$ or US-6484946-\$ or	US-PGPUB;	17:50
	US-6488211-\$ or US-6505193-\$ or	EPO; JPO;	
	US-6507904-\$ or US-6510983-\$ or	DERWENT;	
	US-6542610-\$ or US-6633981-\$ or	IBM_TDB	
	US-6643374-\$ or US-6647494-\$ or		
	US-6659354-\$ or US-6678825-\$ or		
	US-6687721-\$ or US-6697489-\$ or		
	US-6700902-\$ or US-6641045-\$ or		
	US-6629244-\$ or US-6633963-\$ or		
	US-6401208-\$ or US-6389537-\$ or		
	US-6425522-\$ or US-6427909-\$ or		
	US-6427910-\$ or US-6571335-\$).did. or		
	(US-6575372-\$ or US-6603857-\$ or	· ·	
	US-6389533-\$ or US-6357665-\$ or		
	US-6385723-\$ or US-6357004-\$ or		
	US-6202150-\$ or US-6209098-\$ or		
	US-6219423-\$ or US-6220510-\$ or		
	US-6230267-\$ or US-6233685-\$ or		
	US-6260172-\$ or US-6293470-\$ or		
	US-6297789-\$ or US-6317832-\$ or		
	US-6320964-\$ or US-6328217-\$ or		
	US-6354489-\$ or US-6125452-\$ or		
İ	US-6145739-\$ or US-6151677-\$ or		
	US-6151678-\$ or US-6164549-\$ or		
	US-6167551-\$ or US-6181803-\$ or		
	US-6189787-\$).did. or (US-6014442-\$ or		
	US-6021201-\$ or US-6052784-\$ or		
	US-6058478-\$ or US-6070148-\$ or		
	US-6076162-\$ or US-6088450-\$ or		
	US-6091817-\$ or US-6095412-\$ or		
	US-6115816-\$ or US-6122625-\$ or		
	US-5905245-\$ or US-5912453-\$ or		
	US-5923018-\$ or US-5949881-\$ or		
	US-5974143-\$ or US-6000608-\$ or		
	US-5682027-\$ or US-5805712-\$).did. or		
	(US-6145739-\$ or US-5682027-\$ or		
	US-5805712-\$).did.) and (symmetr\$3		
	asymmetr\$4) (public and secret)		

-	38	((US-6427911-\$ or US-6431443-\$ or	USPAT;	2004/04/27
		US-6453397-\$ or US-6484946-\$ or	US-PGPUB;	17:50
		US-6488211-\$ or US-6505193-\$ or	EPO; JPO;	
		US-6507904-\$ or US-6510983-\$ or	DERWENT;	
		US-6542610-\$ or US-6633981-\$ or	IBM_TDB	
		US-6643374-\$ or US-6647494-\$ or	_	
		US-6659354-\$ or US-6678825-\$ or		
		US-6687721-\$ or US-6697489-\$ or		
		US-6700902-\$ or US-6641045-\$ or		
		US-6629244-\$ or US-6633963-\$ or		
		US-6401208-\$ or US-6389537-\$ or	}	
		US-6425522-\$ or US-6427909-\$ or		1
		US-6427910-\$ or US-6571335-\$).didor		
		,	· ·	
		(US-6575372-\$ or US-6603857-\$ or		
		US-6389533-\$ or US-6357665-\$ or		
		US-6385723-\$ or US-6357004-\$ or		
		US-6202150-\$ or US-6209098-\$ or		
		US-6219423-\$ or US-6220510-\$ or		
		US-6230267-\$ or US-6233685-\$ or		
		US-6260172-\$ or US-6293470-\$ or		
		US-6297789-\$ or US-6317832-\$ or		
	1	US-6320964-\$ or US-6328217-\$ or		
	1	US-6354489-\$ or US-6125452-\$ or		
	1	US-6145739-\$ or US-6151677-\$ or		
	1	US-6151678-\$ or US-6164549-\$ or		
	1	US-6167551-\$ or US-6181803-\$ or]
	1	US-6189787-\$).did. or (US-6014442-\$ or		
	1	1		
		US-6021201-\$ or US-6052784-\$ or	İ	
		US-6058478-\$ or US-6070148-\$ or		
		US-6076162-\$ or US-6088450-\$ or		
		US-6091817-\$ or US-6095412-\$ or		
		US-6115816-\$ or US-6122625-\$ or		
		US-5905245-\$ or US-5912453-\$ or		
		US-5923018-\$ or US-5949881-\$ or		
		US-5974143-\$ or US-6000608-\$ or		
		US-5682027-\$ or US-5805712-\$).did. or		
		(US-6145739-\$ or US-5682027-\$ or		
		US-5805712-\$).did.) and ((symmetr\$3		
		asymmetr\$4) (public and secret))	1	
_	0		IICDAM.	2004/04/29
		oozizoi.pii. and chos	USPAT;	1 ' '
	ļ		US-PGPUB;	11:19
	İ		EPO; JPO;	
			DERWENT;	
1			IBM_TDB	
-	1	6021201.pn. and serial	USPAT;	2004/04/29
	1		US-PGPUB;	11:44
1			EPO; JPO;]
1	1		DERWENT;	
1	1		IBM TDB	
-	1	6021201.pn. and (fpga gate or array)	USPAT;	2004/04/29
1	Ī		US-PGPUB;	13:16
	1		EPO; JPO;	
	i		DERWENT;	
	1		IBM TDB	1
_	^	6021201.pn. and eeprom	USPAT;	12004/04/20
	I	oursor, but and cebrom		2004/04/29
1	1		US-PGPUB;	13:16
1	I		EPO; JPO;	
	1		DERWENT;	
	_	6001001	IBM_TDB	
-	0	6021201.pn. and flash	USPAT;	2004/04/29
	1		US-PGPUB;	13:16
	I		EPO; JPO;	
	1		DERWENT;	
	1		IBM TDB	į i
-	0	6021201.pn. and nonvolatile	USPĀT;	2004/04/29
	1	<u> </u>	US-PGPUB;	13:19
	1		EPO; JPO;	
	1		DERWENT;	
	1		IBM TDB]
L	L		TDM IND .	<u> </u>

-	661	(((flash adj memory) or eeprom or prom)	USPAT;	2004/04/29
		same (bus interface) same (sram or dram))	US-PGPUB;	13:24
		and (crypto\$ or cipher encrypt\$3)	EPO; JPO;	
			DERWENT;	
			IBM TDB	
_	184	(((flash adj memory) or eeprom or prom)	USPAT;	2004/04/29
		same (bus interface) same (sram or dram))	US-PGPUB;	13:25
		and (crypto\$ or cipher encrypt\$3) and dma	EPO; JPO;	13.20
		, , , , , , , , , , , , , , , , , , ,	DERWENT;	
			IBM TDB	
_	62	(((flash adj memory) or eeprom or prom)	USPAT;	2004/04/29
		same (bus interface) same (sram or dram))	US-PGPUB;	13:46
		and (crypto\$ or cipher encrypt\$3) and dma	EPO; JPO;	13.40
		and cmos	DERWENT;	
			IBM TDB	
_	221	(((flash adj memory) or eeprom or prom)	USPAT;	2004/04/29
		same (bus interface) same (sram or dram))	US-PGPUB;	13:50
		and (crypto\$ or cipher encrypt\$3) and	EPO; JPO;	13.30
		cmos	DERWENT;	
		Cinob	IBM TDB	
_	37	((((flash adj memory) or eeprom or prom)	USPAT;	2004/04/29
		same (bus interface) same (sram or dram))	US-PGPUB;	13:47
		and (crypto\$ or cipher encrypt\$3) and	EPO; JPO;	13.47
		cmos) and intel	DERWENT;	
		omoby and inter	IBM TDB	
_	482	cmos with key	USPAT;	2004/04/29
	102	omos with key	US-PGPUB;	16:33
			EPO; JPO;	10.33
			DERWENT;	
			IBM TDB	
_	81	cmos with key with (contain\$3 stor\$3	USPAT;	2004/04/29
		sav\$3)	US-PGPUB;	16:42
		54775/	EPO; JPO;	10.42
			DERWENT;	
			IBM TDB	
_	4	(cmos with key with (contain\$3 stor\$3	USPAT;	2004/04/29
		sav\$3)) same reset\$4	US-PGPUB;	16:43
		Saviol' Same Tesechi	EPO; JPO;	10.43
			DERWENT;	
			IRM TOR	

TDB-ACC-NO:

NB910934

DISCLOSURE TITLE: Cryptographic Microcode Loading

Controller for Secure

Function.

PUBLICATION-DATA: IBM Technical Disclosure Bulletin,

September 1991, US

VOLUME NUMBER: 34

ISSUE NUMBER: 4B

PAGE NUMBER: 34 - 36

PUBLICATION-DATE: September 1, 1991 (19910901)

CROSS REFERENCE: 0018-8689-34-4B-34

DISCLOSURE TEXT:

- This article describes a method of implementing a

single-chip microcontroller such that microcode may be loaded, when

desirable, in a secure way.

- The ability to load microcode into a microcontroller at IPL is

advantageous in that one device could be used in a large number of

applications, reducing inventory and cost. Microcode updates could be

installed without having to change physical hardware. This also has

inventory and cost-saving implications.

- An obstacle to this approach, however, is that many

manufacturers of microcontrollers consider the microcode proprietary

and do not wish to have it exposed in plain text while awaiting

loading. For example, the microcode which implements a disk or LAN

controller on a common microcontroller is valuable. If the microcode

is made public by ex posing it in plain text in open

storage or on

disk, it could simply be copied and used elsewhere. This article

describes a method by which microcode could be kept in open storage,

protected by encryption, and then loaded into the microcontroller at

IPL, where it is decrypted for use.

- In a typical microcontroller, a microprocessor executes

microcode out of a Read-Only Memory (ROM), has some data storage

(RAM), and reads and writes from some I/O (which is how it connects

to the device(s) that it is controlling). The important part, for

this discussion, is the microcode ROM. In typical applications the

microcode ROM is masked into the microcontroller during fabrication.

This effectively turns a general-purpose device into a special-purpose device. At the point where the microcode becomes

fabricated into the part, the microcontroller becomes a DASD

controller or a LAN adapter, etc., and can no longer be changed or

upgraded.

- One way of fixing the problem is to use loadable microcode.

This permits a general-purpose device to be customized or updated by

writing new or additional microcode. The problem with this, as was

mentioned previously, is one of security. If the microcode is

exposed in a public area of the system in which the controller is

used, it can be copied or changed without authorization. One solution

is to encrypt the microcode for transportation and storage, and

decrypt it only within the confines of the microcontroller itself.

- Fig. 1 shows a block diagram of this type of system. The

microprocessor, I/O, and RAM remain unchanged. The microcode ROM is

now split into two segments (both ROM and RAM or EEPROM), and a new

storage element (key storage) is defined. The microcode ROM is now a

smaller ROM which would be common to all devices. This smaller ROM

would have bootstrap and decryption microcode, and be used for

initializing and IPLing the microcontroller.

- On power-up, reset, or specific command, this common part of

the ROM would load encrypted microcode into a microcode RAM or

EEPROM, decrypt it, and begin execution. The microcode could be

loaded on existing I/O lines or use a dedicated load path if desired.

To allow the decryption of the microcode, the microcontroller must

have the decryption key for the code. This would be kept in the key

storage element (RAM or EEPROM).

- Both the key storage and the microcode RAM or EEPROM (once it

has been loaded) contain valuable information (the microcode) or the

means to get it (the decryption key), so additional security measures

should be applied. The microcontroller should be fabricated on a

single chip. This prevents probing inter-chip connections. The chip

on which the microcontroller is fabricated should be securely

encapsulated during packaging. Secure encapsulation is a process by

which the chip is coated with a material which obscures the surface

of the chip such that it cannot be effectively examined or probed,

and if removal is attempted, the chip will be ruined, preventing

access to secure data. To provide an additional level of security,

the key store and the microcode store could be CMOS RAM.

This would

make probing or examination more difficult because of

CMOS's

sensitivity to light and static charge. These RAMs could be backed

with a battery when the system was unpowered (in the same manner as

any CMOS RAM). This is a common and inexpensive technique.

- The result would be a general-purpose interface/microcontroller

which could securely load microcode for which it had the decryption

key. Some of the advantages of such a system are:

1. A common device could replace a number of customized

devices. This is desirable from an inventory and stocking

perspective.

- 2. Hardware devices could be field updated in microcode,

without replacing hardware.

- 3. Microcode would become loadable and replaceable, without

becoming vulnerable.

- 4. Microcode upgrades could be sold for added value.

- The subject of key distribution and management is quite

complicated and has not been dealt with here. There are, however,

defined methods of key distribution which are appropriate for this type of system.

SECURITY: Use, copying and distribution of this data is subject to the

restictions in the Agreement For IBM TDB Database and Related Computer

Databases. Unpublished - all rights reserved under the Copyright Laws of the

United States. Contains confidential commercial information of IBM exempt

from FOIA disclosure per 5 U.S.C. 552(b)(4) and protected under the Trade

Secrets Act, 18 U.S.C. 1905.

COPYRIGHT STATEMENT: The text of this article is Copyrighted (c) IBM Corporation 1991. All rights reserved.

To Controlled Device Device Micro-Code Data RAM or EEPROM Key Micro-**Processor** Micro-Code Load Path (optional)

Cryptographic Micro-controller Block Diagram